PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-018855
(43)Date of publication of application : 19.01.2001

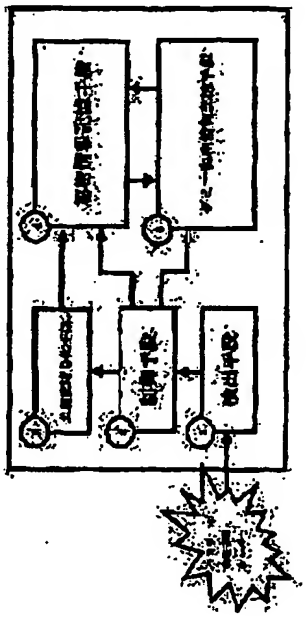
(51)Int.Cl. H04Q 7/38
H04L 9/10
H04M 1/66
H04M 1/67

(21)Application number : 11-184878
(22)Date of filing : 30.06.1999

(71)Applicant : ADVANCED MOBILE TELECOMMUNICATIONS SECURITY TECHNOLOGY RESEARCH LAB CO LTD
(72)Inventor : ANZAI JUN
KATO TAKEHIKO
MATSUZAKI NATSUME
ITO SATORU

(54) PORTABLE TERMINAL WITH SECURITY

(57)Abstract:
PROBLEM TO BE SOLVED: To find out pretender who claims to be a processor of a portable terminal and leakage of secrecy information by always protecting the secrecy information of the portable terminal.
SOLUTION: A secrecy information storage means 4 stores secrecy information of the portable terminal. Furthermore, a dummy secrecy information storage means 5 stores dummy secrecy information. When a detection means 1 detects the number of failures in password entry in excess of processing value or a temper attack, the detection means 1 outputs an attack control signal to a control means 2. Upon the receipt of the attack detection section, the control means 2 transmits an encryption signal to a public key encryption means 3. The public key encryption means 3 uses a public key in a public key encryption to encrypt the secrecy information. The control means 2 deletes the secrecy information and replaces the encrypted secrecy information with the dummy secrecy information.



* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The block diagram of the personal digital assistant equipment in the gestalt of operation of the 1st of this invention,
[Drawing 2] Other block diagrams of the personal digital assistant equipment in the gestalt of operation of the 1st of this invention,
[Drawing 3] Service provision structure-of-a-system drawing using the personal digital assistant equipment in the gestalt of operation of the 2nd of this invention,
[Drawing 4] The block diagram of conventional personal digital assistant equipment,
[Drawing 5] It is the block diagram of another conventional personal digital assistant equipment.
[Description of Notations]
1 Detection Means
2 Control Means
3 Public-Key-Encryption Means
4 Secrecy Information Storage Means
5 Dummy Secrecy Information Storage Means
6 Common Key Encryptosystem-ized Means
10 Personal Digital Assistant Equipment
11 Server or Base Station
12 Blacklist

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] However, in the personal digital assistant equipment of drawing 4, it is that both read the storage section by the tamper since the enciphered confidential information and the cryptographic key used for encryption/decode exist in personal digital assistant equipment, the cipher and the cryptographic key could come to hand, and it had the problem that confidential information was revealed.
[0007] Moreover, unjust opening was detected in the personal digital assistant equipment of drawing 5, and since confidential information was lost while safety can be maintained by eliminating the confidential information memorized, it had the problem that it is difficult to reuse after collecting personal digital assistant equipment, and the problem that confidential information was revealed when opening cannot be detected.
[0008] Although secrecy protection of information was performing any conventional personal digital assistant equipment, leakage of spoofing or individual humanity news was not found, but it had the problem that an inaccurate analyst could not be pursued, either until it suffered damage.
[0009] This invention solves the above-mentioned conventional problem, always protects confidential information, and aims at offering the personal digital assistant equipment which can discover leakage of spoofing or confidential information.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] So that clearly from the above explanation in this invention The secrecy information storage section which memorizes confidential information for personal digital assistant equipment, and a dummy secrecy information storage means to memorize dummy confidential information, A public-key-encryption-ized means to encipher confidential information with the public key of public key encryption, A detection means to detect that the count of failure of a password exceeded constant value, or a tamper, and to output a detecting signal, In response to a detecting signal, an encryption signal is transposed to a public-key-encryption-ized means, delivery and confidential information are transposed to encryption confidential information, confidential information is eliminated, and since it considered as the configuration possessing the control means which replaces encryption confidential information and dummy confidential information, the effectiveness that confidential information can be protected is acquired.
[0038] Moreover, the list which indicated the personal-digital assistant equipment corresponding to dummy confidential information and dummy confidential information to the server of the service provision system which consists of personal digital assistant equipment and a server, Since it had a means by which service was not permitted when it became clear that it is in agreement with a means [list / confidential information / which was transmitted from personal digital assistant equipment] and the dummy confidential information confidential information was indicated to be by the list The effectiveness that an inaccurate terminal user can be detected and service can be refused is acquired.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art] Generally, personal digital assistant equipments, such as a cellular phone, PDA, and an IC card, have confidential information, such as authentication information (a password, personal identification number, etc.) and individual humanity news (address book etc.), in the interior. When personal digital assistant equipments, such as a cellular phone, PDA, and an IC card, are lost or a theft is suited, unjust analysis (tamper) of internal confidential information may be performed. If authentication information is analyzable in unjust analysis, a fixed period becomes completely and ** is possible until loss and a theft are told to a service manager. There may also be leakage of individual humanity news. Even if personal digital assistant equipment was recoverable after loss and a theft, the tamper may have been suited and anxiety arises to use the personal digital assistant equipment.
[0003] As conventional personal digital assistant equipment which can protect confidential information, what was indicated by a publication-number No. 271107 [ten to] official report and JP,9-261217,A is known. The configuration of personal digital assistant equipment given in a publication-number No. 271107 [ten to] official report is shown in drawing 4 . The configuration of personal digital assistant equipment given in JP,9-261217,A is shown in drawing 5 R> 5.
[0004] The personal digital assistant equipment shown in drawing 4 is the security section prepared in the interior of a computer card, and protects confidential information by enciphering and saving confidential information. In a control section and the random-number-generation section, a necessary cryptographic key is generated using a random number. The generated cryptographic key is memorized in the cryptographic key storage section. The cipher system which functions corresponding to the generated cryptographic key is beforehand memorized in the cipher system storage section. Cipher processing is performed to the received plaintext data using the memorized cipher system, and encryption data are created in a code / decode section. The created encryption data are memorized in the encryption data storage section.
[0005] Moreover, the personal digital assistant equipment shown in drawing 5 is the individual pocket device which aimed at prevention of the secrecy leakage by the tamper by detecting a tamper and eliminating a private key. According to the directions from the key generation directions section, the key of public key encryption is generated in the random-number-generation section and the cryptographic key generator section. The generated key is stored in the cryptographic key storing section. the plaintext, cipher, or signature sentence inputted from a plaintext, a cipher, and the signature sentence input section -- the cipher-processing section -- a cryptographic key -- using -- encryption -- or it decodes or signs. If an opening detecting element detects opening, the private key stored in the cryptographic key storing section will be eliminated by the elimination directions section.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention] Especially this invention relates to the personal digital assistant equipment which can protect confidential information in the case of loss or a theft about personal digital assistant equipment.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] Especially this invention relates to the personal digital assistant equipment which can protect confidential information in the case of loss or a theft about personal digital assistant equipment.
[0002]
[Description of the Prior Art] Generally, personal digital assistant equipments, such as a cellular phone, PDA, and an IC card, have confidential information, such as authentication information (a password, personal identification number, etc.) and individual humanity news (address book etc.), in the interior. When personal digital assistant equipments, such as a cellular phone, PDA, and an IC card, are lost or a theft is suited, unjust analysis (tamper) of internal confidential information may be performed. If authentication information is analyzable in unjust analysis, a fixed period becomes completely and ** is possible until loss and a theft are told to a service manager. There may also be leakage of individual humanity news. Even if personal digital assistant equipment was recoverable after loss and a theft, the tamper may have been suited and anxiety arises to use the personal digital assistant equipment.
[0003] As conventional personal digital assistant equipment which can protect confidential information, what was indicated by a publication-number No. 271107 [ten to] official report and JP,9-261217,A is known. The configuration of personal digital assistant equipment given in a publication-number No. 271107 [ten to] official report is shown in drawing 4 . The configuration of personal digital assistant equipment given in JP,9-261217,A is shown in drawing 5 R> 5.
[0004] The personal digital assistant equipment shown in drawing 4 is the security section prepared in the interior of a computer card, and protects confidential information by enciphering and saving confidential information. In a control section and the random-number-generation section, a necessary cryptographic key is generated using a random number. The generated cryptographic key is memorized in the cryptographic key storage section. The cipher system which functions corresponding to the generated cryptographic key is beforehand memorized in the cipher system storage section. Cipher processing is performed to the received plaintext data using the memorized cipher system, and encryption data are created in a code / decode section. The created encryption data are memorized in the encryption data storage section.

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem] The secrecy information storage section which memorizes confidential information for personal digital assistant equipment in this invention in order to solve the above-mentioned technical problem, A public-key-encryption-ized means to encipher confidential information with the public key of public key encryption, It considered as the configuration possessing a detection means to detect that the count of failure of a password exceeded constant value, or a tamper, and to output a detecting signal, and the control means which transposes an encryption signal to a public-key-encryption-ized means, transposes delivery and confidential information to encryption confidential information in response to a detecting signal, and eliminates confidential information. Thus, by having constituted, confidential information is always protected and leakage of spoofing or confidential information can be discovered.
[0011] Moreover, when it became clear that it is in agreement with a means [list / confidential information / the list which indicated the personal digital assistant equipment corresponding to dummy confidential information and dummy confidential information to the server of a service provision system, and / which was transmitted from personal digital assistant equipment], and the dummy confidential information confidential information was indicated to be by the list, it had a means by which service was not permitted. Thus, by having constituted, an inaccurate terminal user is detected and service can be refused.
[0012]
[Embodiment of the Invention] The secrecy information storage section invention of this invention according to claim 1 remembers confidential information to be, A public-key-encryption-ized means to encipher said confidential information with the public key of public key encryption, An attack detection means to detect that the count of failure of a password exceeded constant value, or a tamper, and to output an attack detecting signal, In response to said attack detecting signal, an encryption signal is transposed to said public-key-encryption-ized means, and delivery and said confidential information are transposed to encryption confidential information, and it is personal digital assistant equipment possessing the control means which eliminates said confidential information, and has an operation of performing secrecy protection of information to an inaccurate person's analysis.
[0013] The secrecy information storage section invention of this invention according to claim 2 remembers confidential information to be, A dummy secrecy information storage means to memorize dummy confidential information, and an attack detection means to detect that the count of failure of a password exceeded constant value, or a tamper, and to output an attack detecting signal, It is personal digital assistant equipment possessing the control means which transposes said confidential information to said dummy confidential information in response to said attack detecting signal, and has an operation of enabling it to detect analysis having been performed to an inaccurate person's analysis.
[0014] The secrecy information storage section invention of this invention according to claim 3 remembers confidential information to be, A dummy secrecy information storage means to memorize dummy confidential information, and a public-key-encryption-ized means to encipher said confidential information with the public key of public key encryption, An attack detection means to detect that the count of failure of a password exceeded constant value, or a tamper, and to output an attack detecting signal, Said attack detecting signal is received. An encryption signal for said public-key-encryption-ized means Delivery, Transpose said confidential information to encryption confidential information, and said confidential information is eliminated. It is personal digital assistant equipment possessing the control means which replaces said encryption confidential information and said dummy confidential information, and has an operation of enabling it to detect having protected confidential information to an inaccurate person's analysis, and analysis having been performed.

[0015] In claim 1 and the personal digital assistant equipment of three publications, invention of this invention according to claim 4 establishes a means to obtain said private key from the battery charger which memorized the private key corresponding to said public key, and to decode said encryption confidential information, and has an operation that only a user with a specific battery charger enables it to decrypt encryption confidential information.
[0016] The secrecy information storage section invention of this invention according to claim 5 remembers confidential information to be, A common key encryptosystem-ized means to encipher said confidential information with the common key of a common key encryptosystem, A public-key-encryption-ized means to encipher said common key with the public key of public key encryption, An attack detection means to detect that the count of failure of a password exceeded constant value, or a tamper, and to output an attack detecting signal, Said attack detecting signal is received. An encryption signal for said public-key-encryption-ized means Delivery, Said common key and said confidential information are eliminated, and it is personal digital assistant equipment possessing encryption confidential information and the control means which stores an encryption common key in said secrecy information storage section, and has an operation of reducing the amount of information enciphered with public key encryption, and protecting confidential information at a high speed.
[0017] In the service provision system by which invention of this invention according to claim 6 consists of personal digital assistant equipment and a server according to claim 2 said server The list which indicated the personal digital assistant equipment corresponding to dummy confidential information and said dummy confidential information, A means [said list / confidential information / which was transmitted from said personal digital assistant equipment], When it becomes clear that it is in agreement with the dummy confidential information said confidential information was indicated to be by said list, it is the service provision system equipped with a means by which service is not permitted, and it has an operation of enabling it to detect analysis having been performed by the inaccurate person.
[0018] In the service provision system by which invention of this invention according to claim 7 consists of personal digital assistant equipment and a server according to claim 1 said server The list which indicated the personal digital assistant equipment corresponding to confidential information and said confidential information, A means [said list / decode the encryption confidential information which received with the private key of a public key system, and], When it becomes clear that it is in agreement with the confidential information in said list, it is the service provision system equipped with a means by which service is not permitted, and it has an operation of enabling it to detect analysis having been performed by the inaccurate person.
[0019] In personal digital assistant equipment according to claim 2. said dummy confidential information is information which includes identification information, such as a serial number, and the status information of time of day, a location, etc. at least, and invention of this invention according to claim 8 has an operation of enabling discernment of an unjust terminal.
[0020] Hereafter, the gestalt of operation of this invention is explained to a detail, referring to drawing 1 - drawing 3 .
[0021] (Gestalt of the 1st operation) The gestalt of operation of the 1st of this invention is personal digital assistant equipment which enciphers confidential information with public key encryption, and replaces confidential information with dummy confidential information, when the count of failure of the time of detection of a tamper or a password becomes more than constant value.
[0022] Drawing 1 is the functional block diagram showing the configuration of the personal digital assistant equipment in the gestalt of operation of the 1st of this invention. In drawing 1 R> 1, the detection means 1 is a means to detect that the count of failure of a password exceeded constant value, or a tamper, and to output an attack detecting signal. A control means 2 is a means to transpose an encryption signal to a public-key-encryption-ized means, it to transpose delivery and confidential information to encryption confidential information in response to an attack detecting signal, to eliminate confidential information, and to replace encryption confidential information and dummy confidential information. The public-key-encryption-ized means 3 is a means to encipher confidential information with the public key of public key encryption. The secrecy information storage means 4 is a means to memorize the confidential information of personal digital assistant equipment. The dummy secrecy information storage means 5 is a means to memorize dummy confidential information.
[0023] Drawing 2 is the functional block diagram showing other configurations of the personal digital assistant equipment in the gestalt of operation of the 1st of this invention. In drawing 2 , a control means 2 is a means to

eliminate delivery and a common key for an encryption signal for a public-key-encryption-ized means in response to an attack detecting signal. The public-key-encryption-ized means 3 is a means to encipher a common key with the public key of public key encryption. The secrecy information storage means 4 is a means to memorize the confidential information of personal digital assistant equipment. The common key encryptosystem-ized means 6 is a means to encipher confidential information with a common key.

[0024] Actuation of the personal digital assistant equipment in the gestalt of operation of the 1st of this invention constituted as mentioned above is explained. Generally, since personal digital assistant equipment is performing the activity limit with a password, the inaccurate person who received personal digital assistant equipment first performs the tamper which is going to make personal digital assistant equipment usable, or is going to read confidential information from the secrecy information storage means 4 directly by the exhaustive search attack of a password. The detection means 1 detects this and an attack detecting signal is transmitted.

[0025] The carrier beam control means 2 sends an encryption signal for an attack detecting signal to the public-key-encryption-ized means 3. The confidential information the carrier beam public-key-encryption-ized means 3 was remembered to be by the secrecy information storage means 4 in this encryption signal is enciphered using a public key. A control means 2 eliminates the confidential information of a plaintext, after making the secrecy information storage means 4 memorize this encryption confidential information.

[0026] Finally, a control means 2 replaces the dummy confidential information memorized by the dummy secrecy information storage means 5 and the encryption confidential information memorized by the secrecy information storage means 4. Therefore, the inaccurate person who analyzed the password and made personal digital assistant equipment usable will use it for spoofing etc. by making this dummy confidential information into right confidential information.

[0027] When personal digital assistant equipment is able to be collected, since encryption confidential information is decoded, personal digital assistant equipment can be easily reused only by connecting with the battery charger which memorized the private key. Since there is only a public key in the interior of personal digital assistant equipment, an inaccurate person cannot decode encryption confidential information.

[0028] Next, with reference to drawing 2 , actuation of the personal digital assistant equipment of other configurations in the gestalt of operation of the 1st of this invention is explained. As for public key encryption, generally, since processing speed is slow, when there is much confidential information, encryption takes time amount. So, when a user does not use confidential information, the encryption confidential information which enciphered confidential information by the common key encryptosystem using the common key with the common key encryptosystem-ized means 6 is saved for the secrecy information storage means 4, and the confidential information of a plaintext is eliminated. When the detection means 1 detects an attack, this common key is enciphered with public key encryption using a public key with the public-key-encryption-ized means 3, this encryption common key is saved, and a common key is eliminated. By the above approach, even if confidential information increases, confidential information can be protected at a high speed. However, whenever a user uses confidential information, he needs to decode encryption confidential information, but since a common key encryptosystem is a high speed, it is satisfactory practically.

[0029] As mentioned above, with the gestalt of operation of the 1st of this invention, since it considered as the configuration which enciphers confidential information with public key encryption, and replaces confidential information with dummy confidential information when the count of failure of the time of detection of a tamper or a password became about personal digital assistant equipment more than constant value, the confidential information of personal digital assistant equipment can be protected certainly.

[0030] (Gestalt of the 2nd operation) The gestalt of operation of the 2nd of this invention is a service provision system which has the server which does not permit service, when it becomes clear that it is in agreement with the dummy confidential information with which compared the list which indicated the personal digital assistant equipment corresponding to dummy confidential information and dummy confidential information, and the confidential information transmitted from personal digital assistant equipment, and confidential information was indicated to be by the list.

[0031] Drawing 3 is the functional block diagram showing the configuration of the personal digital assistant equipment in the gestalt of operation of the 2nd of this invention. In drawing 3 R> 3, personal digital assistant equipment 10 is a terminal unit explained with the gestalt of the 1st operation. A server (or base station) 11 is a system which offers service based on the confidential information from a terminal. A blacklist 12 is a list which indicated an unjust terminal and its confidential information.

[0032] Actuation is explained about the service provision system in the gestalt of operation of the 2nd of this

invention constituted as mentioned above, referring to drawing 3 . An inaccurate person is going to perform spoofing using personal digital assistant equipment 10. At this time, confidential information was changed to dummy confidential information. In Step1, in case service is required of a server 11, dummy confidential information will be used as authentication information.

[0033] Next, the server 11 of which service was required checks that compare with a blacklist 11 the authentication information sent by the inaccurate person, and dummy confidential information has been sent. Therefore, since getting to know that spoofing was performed cuts a server 11, it does not permit service.

[0034] In the above explanation, confidential information was transposed to the dummy confidential information currently prepared beforehand. However, when the public key of a server 11 is inputted into personal digital assistant equipment and the detection means 1 detects an attack beforehand, confidential information can be enciphered in a open code using the public key of the server 11, and encryption confidential information can also be used as a substitute of dummy confidential information. In this case, it is a server 11, it decodes using the private key corresponding to the public key of a server 11, and as compared with the decoded confidential information and the confidential information of a customer list, if in agreement, it can judge that encryption confidential information is inaccurate. By this approach, while there is a merit that it is not necessary to prepare a blacklist, cipher processing is needed by the server 11.

[0035] Moreover, since the time amount to which injustice was carried out by using the information (serial number of the location and personal digital assistant equipment of time of day and personal digital assistant equipment) which can specify personal digital assistant equipment as dummy confidential information, the location in, etc. become clear, it becomes easy to pursue an inaccurate person.

[0036] As mentioned above, the gestalt of operation of the 2nd of this invention compares the list which indicated the personal digital assistant equipment corresponding to dummy confidential information and dummy confidential information for a service provision system, and the confidential information transmitted from personal digital assistant equipment, and since it considered as the configuration which has the server which does not permit service when it became clear that it is in agreement with the dummy confidential information confidential information was indicated to be by the list, an unjust terminal is detectable.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The personal digital assistant equipment characterized by to provide the secrecy information-storage section which memorizes confidential information, a public-key-encryption-ized means encipher said confidential information with the public key of public key encryption, an attack detection means detects that the count of failure of a password exceeded constant value, or a tamper, and output an attack detecting signal, and the control means that transposes an encryption signal to said public-key-encryption-ized means, transpose delivery and said confidential information to encryption confidential information in response to said attack detecting signal, and eliminate said confidential information.
[Claim 2] Personal digital assistant equipment characterized by providing the secrecy information storage section which memorizes confidential information, a dummy secrecy information storage means to memorize dummy confidential information, an attack detection means to detect that the count of failure of a password exceeded constant value, or a tamper, and to output an attack detecting signal, and the control means that transposes said confidential information to said dummy confidential information in response to said attack detecting signal.
[Claim 3] The secrecy information storage section which memorizes confidential information, and a dummy secrecy information storage means to memorize dummy confidential information, A public-key-encryption-ized means to encipher said confidential information with the public key of public key encryption, An attack detection means to detect that the count of failure of a password exceeded constant value, or a tamper, and to output an attack detecting signal, Personal digital assistant equipment characterized by providing the control means which transposes an encryption signal to said public-key-encryption-ized means, transposes delivery and said confidential information to encryption confidential information in response to said attack detecting signal, eliminates said confidential information, and replaces said encryption confidential information and said dummy confidential information.
[Claim 4] Claim 1, personal digital assistant equipment of three publications which are characterized by establishing a means to obtain said private key from the battery charger which memorized the private key corresponding to said public key, and to decode said encryption confidential information.
[Claim 5] The secrecy information storage section which memorizes confidential information, and a common key encryptosystem-ized means to encipher said confidential information with the common key of a common key encryptosystem, A public-key-encryption-ized means to encipher said common key with the public key of public key encryption, An attack detection means to detect that the count of failure of a password exceeded constant value, or a tamper, and to output an attack detecting signal, Personal digital assistant equipment characterized by eliminating delivery, and said common key and said confidential information for an encryption signal for said public-key-encryption-ized means in response to said attack detecting signal, and providing encryption confidential information and the control means which stores an encryption common key in said secrecy information storage section.
[Claim 6] In the service provision system which consists of personal digital assistant equipment and a server according to claim 2 said server The list which indicated the personal digital assistant equipment corresponding to dummy confidential information and said dummy confidential information, The service provision system characterized by having a means by which service is not permitted when it becomes clear that it is in agreement with a means [said list / confidential information / which was transmitted from said personal digital assistant equipment] and the dummy confidential information said confidential information was indicated to be by said list.
[Claim 7] It is the service provision system characterized by to have a means do not permit service when it

becomes clear that it is in agreement with the list with which said server indicated the personal digital assistant equipment corresponding to confidential information and said confidential information in the service provision system which consists of personal digital assistant equipment and a server according to claim 1, a means [said list / decode the encryption confidential information which received with the private key of a public key system, and], and the confidential information in said list.

[Claim 8] Said dummy confidential information is personal digital assistant equipment according to claim 2 characterized by being the information which includes identification information, such as a serial number, and the status information of time of day, a location, etc. at least.

[Translation done.]

LEGAL STATUS

[Date of request for examination]	24.03.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	dismissal
[Date of final disposal for application]	28.01.2003
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	